AN: PAT 1986-138240
TI: Input-output failure protection for multiprocessor system transmitting data over duplicated channels with facility to identify faulty unit
PN: DE3442418-A
PD: 22.05.1986
AB: The multiprocessor has duplicated redundancy built in to provide safe operation. A number of processors (RS1-RS6) have duplicated input/output units (E/A21, E/A22, etc.) that are led to two buses (B1, B2). A digital data from one processor (RS2) to another (RS1) is either transmitted in identical form or in true and inverted form by the I/O stages (E/A21, E/A22). Upon reception the data is subjected to a checking procedure. Any fault in the I/O unit is signalled back to the transmitting processor. Any further transmissions are switched to an alternative processor that has correctly operating I/O units.; To control railway network switching system.
PA: (SIEI) SIEMENS AG;
IN: GUNTHER R; LOHMANN H J;
FA: DE3442418-A 22.05.1986; DE3585361-G 19.03.1992; **EP182134**-A 28.05.1986; **EP182134**-B 05.02.1992;
CO: AT; CH; DE; EP; LI; NL;
DR: AT; CH; DE; LI; NL;
IC: G06F-011/16;
MC: T01-G03; T01-H01; T01-J02;
DC: T01;
PR: DE3442418 20.11.1984;
FP: 22.05.1986
UP: 19.03.1992

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 182 134**
A2

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **85113416.3**

(22) Anmeldetag: **22.10.85**

(51) Int. Cl.⁴: **G 06 F 11/00**

(30) Priorität: **20.11.84 DE 3442418**

(43) Veröffentlichungstag der Anmeldung: **28.05.86**
Patentblatt 86/22

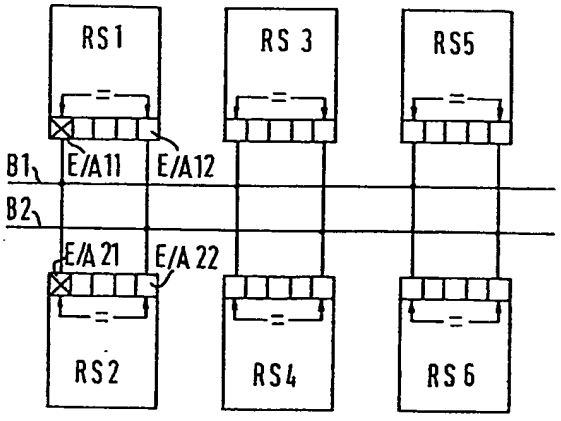
(84) Benannte Vertragsstaaten: **AT CH DE LI NL**

(71) Anmelder: **Siemens Aktiengesellschaft, Berlin und München Wittelsbacherplatz 2, D-8000 München 2 (DE)**

(72) Erfinder: **Lohmann, Heinz-Jürgen, Dr.-Ing., Erftstrasse 10, D-3300 Braunschweig (DE)**
Erfinder: **Günther, Rudolf, Dipl.-Ing., Ackerweg 25, D-3300 Braunschweig (DE)**

(54) Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mehreren signaltechnisch nicht sicheren Ein/Ausgabebaugruppen.

(57) Das Mehrrechnersystem (RS1) prüft laufend die in den Ein/Ausgabebaugruppen (E/A11, E/A12) seiner Einzelrechner anstehenden, über gesonderte Kanäle übermittelten Daten auf Übereinstimmung. Beim Auftreten von Abweichungen führt das Mehrrechnersystem Redundanzprüfungen durch und ermittelt aus dem Ergebnis dieser Prüfungen die jeweils defekte Ein/Ausgabebaugruppe (z.B. E/A11). Für eine bestimmte Zeitspanne wird der Datenverkehr dann über eine noch intakte Ein/Ausgabebaugruppe (E/A12) abgewickelt. Die Datenübertragung während dieser Zeit erfolgt höherredundant als bei ordnungsgerechtem Zustand aller Ein/Ausgabebaugruppen.



EP 0 182 134 A2

Siemens Aktiengesellschaft
Berlin und München

Unser Zeichen
VPA 84 P 2938 E

Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mehreren signaltechnisch nicht sicheren Ein/Ausgabebaugruppen

Die Erfindung bezieht sich auf ein Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mindestens zwei signaltechnisch nicht sicheren Ein/Ausgabebaugruppen, über die die Rechner des Mehrrechnersystems mindestens zweikanalig Datentelegramme von und/oder zu anderen Rechnern und/oder sonstigen Daten aufnehmenden, abgebenden oder verarbeitenden Schaltmitteln übertragen und über die sie von dort in Form von inhaltlich übereinstimmenden Telegrammen für die Ein/Ausgabebaugruppen durch Prüfdaten gesicherte Nutzdaten empfangen bzw. nach dort abgeben.

Für besonders sicherheitsrelevante Anwendungsfälle wie z.B. das Eisenbahnsicherungswesen sind signaltechnisch sichere Mehrrechnersysteme entwickelt worden, in denen die zu verarbeitenden Daten in mehreren Kanälen jeweils unabhängig voneinander nach bestimmten Gesetzmäßigkeiten behandelt werden; durch Vergleichsprozeduren werden etwaige Datenabweichungen in den einzelnen Kanälen erkannt und in entsprechende Steuerkommandos umgesetzt, die im Sinne eines Gefährdungsausschlusses auf den zu steuernden Prozeß wirken. Signaltechnisch sichere Mehrrechnersysteme müssen aber nicht nur in der Lage sein, die ihnen zugeführten Daten in der vorgegebenen Weise zu behandeln, sondern sie müssen auch in der Lage sein festzustellen, ob die in ihren signaltechnisch nicht

sicheren Ein/Ausgabebaugruppen anstehenden Daten beispielsweise infolge einer Übertragungsstörung oder eines Bauteiledefektes verfälscht sind oder nicht, um dann die Auswertung dieser verfälschten Daten zu unterbinden.

Ein bekanntes Verfahren zur Sicherung der Datenübermittlung sieht vor, den eigentlichen Nutzdaten sendeseitig nach bestimmten Gesetzmäßigkeiten gebildete Prüfdaten beizugeben, aus den übermittelten Nutzdaten empfangsseitig nach den gleichen Gesetzmäßigkeiten die zugehörigen Prüfdaten nachzubilden und diese mit den übermittelten Prüfdaten zu vergleichen. Diese Art der Datensicherung ist im allgemeinen um so wirkungsvoller, je aufwendiger die Prüfdaten werden.

Bei der heutigen Technik sind die Ein/Ausgabebaugruppen elektronischer Datenverarbeitungseinrichtungen üblicherweise mit hochintegrierten Schaltkreisen (FIFOS) besetzt, deren mögliche Ausfallreaktionen nicht umfassend bekannt sind und aus Aufwandsgründen auch nicht durch Analyse ermittelt werden können. Dies hat zur Folge, daß der Nachweis dafür, daß es keine Ausfallwirkung gibt, die trotz Redundanzprüfung unerkannt bleibt, in letzter Konsequenz nicht vollständig geführt werden kann, so daß auch bei sehr umfangreichen Prüfdaten nicht erkennbare Nutzdatenverfälschungen nicht ausgeschlossen werden können. Deshalb erfüllt dieses Lösungskonzept die Forderungen hinsichtlich signaltechnischer Sicherheit als Voraussetzung für die Zulassung einer Telegrammübertragung für besonders sicherheitsrelevante Anwendungen nur unzureichend.

Nicht vorhersagbare Ausfallreaktionen einer Baugruppe, z.B. einer mit hochintegrierten Schaltkreisen bestückten

Ein/Ausgabebaugruppe, lassen sich grundsätzlich durch Vervielfachung dieser Baugruppen und Vergleich ihrer Reaktionen miteinander erkennen. Für den vorliegenden Anwendungsfall bedeutet dies, daß die ein-bzw. auszugebenden Informationen jeweils parallel in mindestens zwei gesonderte Ein/Ausgabebaugruppen einzuschreiben sind und daß das Mehrrechnersystem dann die gegenseitige Übereinstimmung der abgespeicherten Daten überprüft. Wird beim Vergleich der in diesen Baugruppen gespeicherten Daten eine Ungleichheit erkannt, so sperrt das Rechnersystem die Verwertung der gespeicherten Informationen. Damit ist die Ungefährlichkeit des ersten Ausfalls einer Ein/Ausgabebaugruppe absolut gegeben.

Ein Defekt an einer Ein/Ausgabebaugruppe soll zwar als solcher sofort erkannt und in seiner Auswirkung unwirksam gemacht werden; ein derartiger Defekt soll jedoch nach Möglichkeit nicht den weiteren Datenverkehr des Rechnersystems mit den Systemelementen blockieren, die die durch den Defekt betroffene Ein/Ausgabebaugruppe mit Daten versorgen bzw. von dort Daten beziehen und er soll insbesondere nicht zum Ausfall des gesamten Rechnersystems führen. Um den Datenverkehr auch beim Ausfallen einzelner Ein/Ausgabebaugruppen fortführen zu können, ist es bekannt, jeder Ein/Ausgabebaugruppe mindestens eine entsprechende Reservebaugruppe beizuordnen, die spätestens im Störungsfall zu aktivieren ist und dann die Datenübertragung übernimmt.

Nachteilig an dieser Ausführung ist der hohe Aufwand für die Ein/Ausgabebaugruppen. Dies ist besonders schwerwiegend, wenn es sich bei den Ein/Ausgabebaugruppen um die Schnittstellen zu vielen anderen Rechnern oder sonstigen Anlagenelementen mit gleichen Anforderungen han-

delt. Dann muß nämlich dieser zusätzliche Aufwand an allen Rechnern getrieben werden und das geht erheblich ins Geld.

Eine Möglichkeit, die beiden vorgenannten Sicherungsmethoden miteinander zu verknüpfen, besteht darin, die zu übermittelnden Daten mit Prüfdaten zu versehen und mehrkanalig auszuwerten. Dieses Verfahren wird bei der in der DE-OS 26 09 107 offenbarten Schaltung angewandt. Nach Prüfung der Redundanz in mehreren voneinander unabhängigen Baugruppen werden die von diesen Baugruppen gebildeten Ergebnisse miteinander verglichen. Wenn man davon ausgeht, daß - wie bereits dargelegt - durch Redundanzprüfungen Datenverfälschungen in einem Register nicht mit absoluter Sicherheit erkannt werden können, dann können derartige Verfälschungen auch nicht durch eine verdoppelte Redundanzprüfung sicher aufgezeigt werden. Das bedeutet, daß die aus der DE-OS 26 09 107 bekannte Schaltung den hohen Sicherheitsanforderungen signaltechnisch sicherer Mehrrechnersysteme nicht gerecht wird.

Aufgabe der vorliegenden Erfindung ist es, Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems gemäß dem Oberbegriff des Patentanspruches 1 bzw. 2 anzugeben, die etwaige Datenverfälschungen in bestimmten, durch inhaltlich gleiche Datentelegramme beschickten Ein/Ausgabebaugruppen sicher erkennen, um sie in ihrer Auswirkung unwirksam zu machen und die es darüber hinaus gestatten , den Datenverkehr auch nach dem Auftreten einer Datenverfälschung mindestens bedingt aufrechtzuerhalten, ohne daß es hierzu der Bereitstellung zusätzlicher Reservebaugruppen bedarf. Die erfindungsgemäßen Verfahren sollen dabei in sich so transparent sein, daß

der Nachweis für den sicheren Aufgriff von Datenverfälschungen als Voraussetzung für die Zulassung der erfindungsgemäßen Verfahren bei sicherheitsrelevanten Anwendungen möglich ist. Ferner ist es Aufgabe der Erfindung, solche Einrichtungen zu benennen, die besonders geeignet sind für die Durchführung der erfindungsgemäßen Verfahren.

Die Erfindung löst diese Aufgabe durch die kennzeichnenden Merkmale des Patentanspruches 1 bzw. die des Patentanspruches 2. Vorteilhafte Aus- und Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

Beide Verfahren sind so beschaffen, daß sie auf in den mit übereinstimmenden Datentelegrammen zu belegenden Ein/Ausgabebaugruppen eines Mehrrechnersystems auftretende Datenverfälschungen sicher reagieren, die Auswertung der fehlerbehafteten Daten verhindern und die an der Datenverfälschung tatsächlich oder möglicherweise beteiligten Elemente von der weiteren Datenübermittlung ausschließen. Dabei führen die beiden Verfahren zu unterschiedlichen Reaktionen bezogen auf die Anzahl der von der jeweiligen Störung betroffenen Systemelemente. Nach beiden Verfahren wird die Datenübertragung im Anschluß an das Auffinden fehlerbehafteter Daten unter zusätzlicher Datensicherung und Belegung eines durch die Datenverfälschung nicht betroffenen Übertragungskanals für eine bestimmte Zeitspanne zugelassen, die zum Beheben des eingetretenen Defektes genutzt werden kann.

Die Erfindung ist nachstehend anhand von in der Zeichnung schematisch dargestellten Ausführungsbeispielen

näher erläutert.

Die Zeichnung zeigt in den Figuren 1 und 2 einen besonders vorteilhaften Aufbau von aus mehreren signaltechnisch sicheren Mehrrechnersystemen bestehenden Rechneranordnungen, die in unterschiedlicher Weise auf fehlerhaft abgelegte Daten reagieren, und in Figur 3 ein Funktionsschaubild zur Erläuterung der erfindungsgemäßen Verfahren bei einem signaltechnisch sicheren Zweirechnersystem.

Die in Figur 1 dargestellte Rechneranordnung besteht aus beispielsweise sechs signaltechnisch sicheren Mehrrechnersystemen RS1 bis RS6, die über zugeordnete Ein/Ausgabebaugruppen an die beiden Busse B1 und B2 eines Bussystems angeschlossen sind, über das die Mehrrechnersysteme zweikanalig miteinander kommunizieren. Es ist angenommen, daß das Rechnersystem RS2 Daten in Form eines Telegrammes an das Rechnersystem RS1 zu übermitteln hat. Hierzu aktiviert das Rechnersystem RS2 seine beiden Ein/Ausgabebaugruppen E/A21 und E/A22 zur beispielsweise adressenorientierten Übertragung inhaltlich gleicher Datentelegramme über die beiden Busse B1 und B2 an die Ein/Ausgabebaugruppen E/A11 und E/A12 des Rechnersystems RS1; die über die beiden Busse übertragenen Datentelegramme können dabei unterschiedlich, z.B. invers dargestellt sein. Das die Daten aufnehmende Rechnersystem RS1 prüft die in seinen Ein/Ausgabebaugruppen abgelegten Daten vor ihrer Anerkennung auf Einhaltung des festgelegten Datenformates und auf inhaltliche Übereinstimmung. Dabei möge das Rechnersystem RS1 in seinen Ein/Ausgabebaugruppen E/A11 und E/A12 voneinander abweichende Daten feststellen. Das Rechnersystem verwirft daraufhin das übermittelte Datentelegramm und fordert über beide

Busse B1, B2 vom Datensender, dem sicheren Mehrrechnersystem RS2, eine erneute Telegrammübertragung an. Genügen die dabei übermittelten Daten den Prüfbedingungen des Rechnersystems RS1, so werden sie anerkannt, wobei die Anerkennung der Daten dem Datensender quittiert werden kann. Endet auch der zweite Versuch einer Datenübermittlung negativ, d.h. stellt der Datenempfänger inhaltlich oder vom Format her abweichende Daten in seinen Ein/Ausgabebaugruppen fest, so stellt er auf noch zu erläuternde Weise fest, welcher der in seinen Ein/Ausgabebaugruppen abgelegten Datensätze fehlerhaft ist und welcher nicht. Im vorliegenden Beispiel möge das Rechnersystem RS1 die in seiner Ein/Ausgabebaugruppe E/A11 anstehenden Daten als fehlerhaft erkannt.haben. Es sperrt daraufhin rechnerintern die weitere Aufnahme von Daten über die betreffende Ein/Ausgabebaugruppe und unterrichtet mindestens das Mehrrechnersystem RS2, von dem das fehlerbehaftete Datentelegramm stammte, hiervon. Dies führt dort zum Setzen eines entsprechenden Sperrvermerkes, der die weitere Übertragung von Daten über die Ein/Ausgabebaugruppe E/A21 zur Ein/Ausgabebaugruppe E/A11 des Mehrrechnersystems RS1 verhindert. Damit wird dem Umstand Rechnung getragen, daß empfangsseitig zwar die aufgetretene Datenverfälschung erkennbar ist, nicht jedoch, wo der Ort dieser Datenverfälschung liegt.

Wenn die von der festgestellten Störung direkt betroffenen beiden Rechnersysteme auch mit anderen, an das gleiche Bussystem angeschlossenen Rechnersystemen kommunizieren sollen, ist es vorteilhaft, auch diese Rechner davon zu unterrichten, daß bestimmte Ein/Ausgabebaugruppen des die Störung feststellenden Rechnersystems und ggf. des Rechnersystems, von dem das verfälschte Datentelegramm stammte, für die weitere Datenübertragung

nicht mehr zur Verfügung stehen. Hierdurch soll verhindert werden, daß ein Defekt in einer einzigen Ein/Ausgabebaugruppe nach und nach zum Sperren weiterer Ein/Ausgabebaugruppen anderer Rechnersysteme führt.

Die durch die Störung direkt betroffenen Mehrrechnersysteme RS1 und RS2 korrespondieren untereinander und ggf. mit den durch die Störung nicht direkt betroffenen Mehrrechnersystemen RS3 bis RS6 fortan auf eine Weise, wie sie im einzelnen anhand der Figur 3 erläutert wird.

Bei dem Ausführungsbeispiel der Figur 2 ist angenommen, daß auch das jeweils sendende Mehrrechnersystem die in seinen Ein/Ausgabebaugruppen zur Übertragung anstehenden Daten vor der Übertragung auf Übereinstimmung prüft. Wieder soll dabei das sichere Mehrrechnersystem RS2 Datentelegramme über das Bussystem B1, B2 an das Mehrrechnersystem RS1 übermitteln. Beim Rücklesen der in den Ein/Ausgabebaugruppen E/A21 und E/A22 anstehenden Daten möge das Mehrrechnersystem RS2 Abweichungen in den Daten feststellen. Die Ausgabe dieser Daten wird daraufhin verhindert und das Rechnersystem versucht - ggf. nach erneuter Generierung der entsprechenden Daten - auf noch zu erläuternde Weise festzustellen, welcher der in seinen Ein/Ausgabebaugruppen anliegenden Datensätze fehlerhaft ist. Es möge dabei zu der Erkenntnis gelangen, daß die in seiner Ein/Ausgabebaugruppe E/A21 anliegenden Daten fehlerhaft sind. Das sichere Mehrrechnersystem veranlaßt daraufhin durch Setzen einer entsprechenden Sperrmarkierung, daß über diese Ein/Ausgabebaugruppe keine weiteren Daten abgegeben werden; ggf. wird auch die Aufnahme von Daten über diese Ein/Ausgabebaugruppe gesperrt. Das Mehrrechnersystem RS2 unterrichtet die übrigen Mehr-

rechnersysteme von dieser Maßnahme und kommuniziert mit diesen Rechnersystemen fortan auf die nachstehend näher erläuterte Weise.

Die Zeichnung zeigt in Figur 3 ein Funktionsschaubild für die Erläuterung der erfindungsgemäßen Verfahren zum Betrieb eines Mehrrechnersystems, das durch zwei Einzelrechner R1 und R2 gebildet wird. In der Zeichnung sind nur diejenigen Elemente dargestellt, die für die Erläuterung der erfindungsgemäßen Verfahren erforderlich sind. Die Ein- bzw. Ausgabe der hier interessierenden Daten erfolgt über zwei signaltechnisch nicht sichere Ein/Ausgabebaugruppen E/A1 und E/A2, die auf gesonderte Busse B1 und B2 geführt sind. Über diese Ein/Ausgabebaugruppen können sowohl Datentelegramme vom Rechnersystem aufgenommen als auch Daten an andere Rechner oder an eine Peripherie abgegeben werden. Die Daten setzen sich aus Nutz- und Prüfdaten zusammen.

Die bei der Eingabe von Daten in das Zweirechnersystem über die Busse B1, B2 zweikanalig angelieferten und in den Registern der Ein/Ausgabebaugruppen E/A1 und E/A2 anstehenden Daten werden im Zweirechnersystem jeweils vor ihrer Anerkennung miteinander verglichen, wobei sich dieser Vergleich zunächst nur auf die Nutzdaten beschränken kann; es ist aber auch möglich, die jeweils übermittelten Daten grundsätzlich auch einer Redundanzprüfung zu unterziehen, d.h. die Zuordnung von Nutz- und Prüfdaten zu prüfen. Dieser Vergleich bzw. die zusätzliche Redundanzprüfung findet dezentral in den beiden Einzelrechnern R1, R2 des sicheren Mehrrechnersystem statt. Jeder Einzelrechner vergleicht bzw. prüft die ihm von beiden Ein/Ausgabebaugruppen E/A1 und E/A2 angebotenen Datensätze. Stellen die Rechner unabhängig voneinander

aber übereinstimmend abweichende Daten in den beiden Ein/Ausgabebaugruppen fest, so verwerfen sie die dort abgelegten Daten und fordern vom jeweiligen Datensender die erneute Übertragung der von ihnen als fehlerhaft erkannten Daten an. Genügen diese Daten den gegebenen Bewertungsbedingungen, so werden sie von den beiden Einzelrechnern akzeptiert und der weiteren Verarbeitung RV1, RV2 zugeführt.

Genügen die angeforderten Daten auch jetzt den gegebenen Bewertungsbedingungen nicht, so werden auch sie verworfen. Die beiden Einzelrechner R1, R2 versuchen nun festzustellen, welche der beiden Ein/Ausgabebaugruppen fehlerhafte Daten enthält und welche nicht. Hierzu unterziehen beide Rechner die ihnen von beiden Ein/Ausgabebaugruppen zugeführten Daten einer Redundanzprüfung. Dabei sollen beide Rechner übereinstimmend feststellen, daß der in einer Ein/Ausgabebaugruppe anstehende Datensatz den Redundanzbedingungen genügt, der andere jedoch nicht. Im angenommenen Fall sollen beide Rechner die in der Ein/Ausgabebaugruppe E/A2 anliegenden Daten als fehlerhaft erkannt haben, während die in der Ein/Ausgabebaugruppe E/A1 anstehenden Daten den vorgegebenen Redundanzbedingungen genügen sollen.

Nach dem Vergleich ihrer Prüfergebnisse veranlassen beide Rechner das Setzen von Sperrmarkierungen und diese Sperrmarkierungen verhindern, daß die in der Ein/Ausgabebaugruppe E/A2 abgelegten Daten mindestens beim Datenverkehr mit demjenigen Element des Übertragungssystems, von dem die Daten fehlerhaft empfangen bzw. abgelegt wurden, fortan ausgewertet bzw. fortgeschaltet werden. Dies geschieht z.B. dadurch, daß rechnerintern der Aufruf der der als gestört erkannten Ein/Ausgabebaugruppe

zugeordneten Adresse verhindert wird.
Das die Störung erkennende Rechnersystem R1, R2 unterrichtet nun über das Bussystem die Datenquelle, von der die die Störung verursachenden Daten stammen, über die eingetretene Störung und den durch die Störung betroffenen Übertragungskanal B1. Die jeweils angesprochene Datenquelle sperrt daraufhin ihrerseits die Auswertung bzw. Fortschaltung von Datentelegrammen über den gestörten Übertragungskanal B1. Die beiden durch die Störung direkt betroffenen Rechnersysteme kommunizieren dann nur noch über mindestens einen durch die Störung nicht betroffenen Übertragungskanal, im angenommenen Beispiel über den Bus B2.
Für den Fall, daß mindestens einer der beiden von der Störung direkt betroffenen Mehrrechnersysteme über das Bussystem noch mit weiteren Rechnersystemen kommunizieren soll, ist es vorteilhaft, auch diese Rechner davon zu unterrichten, daß bestimmte Ein/Ausgabebaugruppen für die Datenübertragung nicht mehr zur Verfügung stehen.
Gleichzeitig mit dem Setzen der Sperrmarkierung fordert das die Störung erkennende Rechnersystem das Rechnersystem, von dem die fehlerbehafteten Daten stammen, bzw. auch alle Rechnersysteme, mit denen es zu kommunizieren hat, dazu auf, zukünftig für die Übertragung von Daten an das Rechnersystem R1, R2 höherredundante Daten zu erstellen und ausschließlich an die Ein/Ausgabebaugruppe E/A1 zu übertragen; entsprechend unterrichtet das sichere Mehrrechnersystem R1, R2 das bzw. die übrigen Mehrrechnersysteme davon, daß es selbst ebenfalls höherredundante Daten erstellen und diese über die Ein/Ausgabebaugruppe E/A1 an die Mehrrechnersysteme übermitteln wird.

Die vorstehend erläuterten Maßnahmen können sinngemäß auch für einen Datensender gelten, von dem die als fehlerhaft erkannten Daten stammen.

Einzelne oder alle Mehrrechnersysteme überprüfen nun fortlaufend bei Datenverkehr mit dem bzw. den durch die Störung direkt betroffenen Mehrrechnersystemen das Einhalten der verschärften Redundanzbedingungen und sie erstellen auch selbst für den Datenverkehr mit diesen Mehrrechnersystemen die höherredundanten Daten. Entsprechendes gilt für die Mehrrechnersysteme mit den ausgefallenen Ein/Ausgabeeinrichtungen.

Eine besonders bevorzugte Ausführungsform der Erfindung sieht vor, daß die nach dem Ausfallen einer Ein/Ausgabebaugruppe zu übertragenden höherredundanten Datentelegramme das gleich Format wie die zuvor übertragenen Datentelegramme aufweisen, daß sie aber von der jeweiligen Datenquelle her mehrfach übertragen werden, wobei sich dann nicht ihr Inhalt aber ihre Darstellung ändert. Vorzugsweise ist dabei an eine inverse Darstellung der Daten in aufeinanderfolgenden Datentelegrammen gedacht. Das jeweils als Empfänger fungierende sichere Mehrrechnersystem prüft vor der Anerkennung der Daten, ob in den ihm nacheinander übermittelten Datentelegrammen sowohl die Nutz- als auch die Prüfinformationen jeweils von ihrem Inhalt her übereinstimmen und ob die übermittelten Prüfinformationen mit den vom Rechnersystem nachgebildeten Prüfinformationen übereinstimmen. Nur solange diese Voraussetzungen gegeben sind, ist die Auswertung der von einem Rechnersystem mit einer defekten Ein/Ausgabebaugruppe stammenden Daten zulässig. Führt eine Redundanzprüfung zu dem Ergebnis, daß entweder die nach-

einander übermittelten Nutz- und Prüfinformationen nicht übereinstimmen oder daß die Zuordnung von Nutz- und Prüfinformationen nicht mehr gegeben ist, so wird der weitere Datenverkehr zum bzw. vom Mehrrechnersystem über die als gestört angesehenen Ein/Ausgabebaugruppen abgebrochen. Das Mehrrechnersystem mit den ausgefallenen Ein/Ausgabebaugruppen schaltet sich aber nur insoweit aus dem Rechnerverbund aus als die Datenübermittlung über die gestörten Ein/Ausgabebaugruppen betroffen ist; im übrigen arbeitet es nach wie vor weiter und setzt über andere Ein/Ausgabebaugruppen zugeführte Meldungen bestimmungsgemäß in entsprechende Kommandos um und überträgt diese Kommandos an die Prozeßperipherie.

Die Fortführung des Datenverkehrs über nur eine von zwei üblicherweise mit inhaltlich gleichen Datentelegrammen versorgte Ein/Ausgabebaugruppen ist nach der Lehre der vorliegenden Erfindung aber nicht für unbegrenzte Zeit zulässig, sondern diese Zeit ist auf eine maximal zulässige Zeitspanne begrenzt. Ist bis zu diesem Zeitpunkt die Störung durch Auswechseln oder Instantsetzen der gestörten Ein/Ausgabebaugruppe bzw. des Übertragungskanals nicht behoben, so verbietet sich die weitere Datenübertragung über das Bussystem. Die maximal zulässige Zeit für das Aufschalten einer einzigen Ein/Ausgabebaugruppe auf beide Einzelrechner des Mehrrechnersystems ist abhängig von der für die betreffende Baugruppe aufgrund ihres Aufbaus zu erwartenden mittleren Zeit zwischen zwei unabhängig voneinander auftretenden Fehlern (MTBF = meantime between failures) und einer Kenngröße, die abhängig ist von der für die Datendarstellung erreichten Redundanz. Die erreichbare maximale Zeit, in der die Telegrammübertragung z.B. einkanalig betrieben werden darf, liegt bei einer typischen Rechneranordnung

mit einer Vielzahl von signaltechnisch sicheren Mehrrechnersystemen in der Größenordnung von weit über 10 Stunden. In dieser Zeit, die rechnerisch bestimmt werden kann, läßt sich der eingetretene Defekt durch Instandsetzung oder durch Ersatz von Baugruppen mühelos beheben.

Für die Begrenzung der Zeitspanne, für die nach dem Ausfallen einer Ein/Ausgabebaugruppe der Datenverkehr über eine noch intakte Ein/Ausgabebaugruppe weitergeführt werden darf, ist dem sicheren Mehrrechnersystem ein signaltechnisch sicheres Zeitglied zugeordnet. Dieses signaltechnisch sichere Zeitglied, das in der Zeichnung durch die Zeitglieder T1 und T2 verdeutlicht ist, wird eingestellt, sobald die Rechner des Mehrrechnersystems die Auswertung der in einer Ein/Ausgabebaugruppe abgespeicherten Daten bleibend verhindern. Wird die dem Zeitglied eingeprägte Schaltzeit überschritten, so sperren die Rechner auch die Auswertung der noch intakten Ein/Ausgabebaugruppe. Diese Sperrung tritt auch ein, wenn mindestens einerder Einzelrechner in den ihm mitgeteilten höherredundanten Daten irgendwelche Fehler entdeckt und wenn diese Fehler nicht durch nochmalige Datenübertragung zu beseitigen sind.

Für die Fortführung des Datenverkehrs nach dem Auftreten einer Störung in einer Ein/Ausgabebaugruppe ist ausschlaggebend, daß das betroffene Mehrrechnersystem die defekte Ein/Ausgabebaugruppe beziehungsweise den gestörten Datenkanal auch tatsächlich erkennt und nicht etwa Daten aus der defekten Ein/Ausgabebaugruppe beziehungsweise aus dem gestörten Datenkanal übernimmt. Wie bereits erläutert wird die defekte und die intakte Ein/Ausgabebaugruppe über Redundanzprüfungen ermittelt.

Dabei kann der Fall eintreten, daß nicht nur eine, sondern beide Redundanzprüfungen zu dem Ergebnis kommen, daß die jeweils übermittelten Prüfdaten mit den vom Mehrrechnersystem nachgebildeten Prüfdaten übereinstimmen. Dies ist möglich, wenn neben der Verfälschung von Nutzdaten im gleichen Kanal auch die übermittelten Prüfdaten gerade so verfälscht werden, daß sich daraus die für die verfälschten Nutzdaten richtigen Prüfdaten ergeben. Dieser Fall ist zwar sehr unwahrscheinlich, er ist jedoch nicht gänzlich auszuschließen. Tritt dieser Fall ein, so wird dies beim Vergleich der Redundanzprüfergebnisse festgestellt. Da die beiden Einzelrechner aus den Redundanzprüfungen in diesem Fall nicht den gestörten Übertragungskanal eindeutig bestimmen können, unterbinden sie in diesem Fall die weitere Datenübertragung über beide Ein/Ausgabebaugruppen.

Die vorstehend für Rechneranordnungen nach Figur 1 beschriebenen Abläufe gelten entsprechend auch für Rechneranordnungen gemäß Figur 2, bei denen die Rechner eines Mehrrechnersystems die in ihren Ein/Ausgabebaugruppen zur Übertragung anstehenden Datentelegramme vor ihrer Freigabe zurücklesen und die Freigabe vom Bilden übereinstimmender Prüfergebnisse in den Rechnern des Mehrrechnersystems abhängig machen.

Die erfindungsgemäßen Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems sind nicht auf die Ausbildung des sicheren Mehrrechnersystems als Zwei-von-Zwei/Rechnersystem beschränkt. Sie lassen sich vielmehr mit Vorteil bei jedem beliebigen signaltechnisch sicheren Mehrrechnersystem anwenden, das über mindestens zwei mit inhaltlich gleichen Datentelegrammen beschickte Ein/Ausgabebaugruppen mit anderen Rechnern oder mit

der Peripherie kommuniziert. Bei einem derartigen aufwendiger gestalteten Mehrrechnersystem kann es zulässig sein, nicht nur den Ausfall einer einzigen Ein/Ausgabebaugruppe, sondern ggf. auch den Ausfall mehrerer Ein/Ausgabebaugruppen zu tolerieren, wenn über die vorhandenen noch intakten Ein/Ausgabebaugruppen ein ordnungsgerechter Datenverkehr noch möglich ist. Die erfindungsgemäßen Verfahren sind insbesondere auch bei einem Zwei-von-Drei/Rechnersystem vorteilhaft anwendbar.

Für die Datenübertragung zwischen den einzelnen Mehrrechnersystemen können beliebige Übertragungssysteme vorgesehen sein; vorzugsweise ist jedoch an die Verwendung linearer Bussysteme, insbesondere Ringbussysteme gedacht.

Dort, wo derartige Übertragungssysteme verdoppelt werden, geschieht dies überwiegend aus Verfügbarkeitsgründen. Bei dem erfindungsgemäßen Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems dagegen wird die Verdoppelung der Bussysteme zunächst ausschließlich zur Erhöhung der Sicherheit beim Datenverkehr zwischen den Rechnersystemen verwendet, indem die Daten mehrkanalig übertragen und die in den Ein/Ausgabebaugruppen jeweils anliegenden Daten vor ihrer Anerkennung auf Übereinstimmung geprüft werden. Erst beim Ausfall eines Übertragungskanals zwischen zwei Mehrrechnersystemen wird die einem verdoppelten Übertragungssystem innenwohnende hohe Verfügbarkeit ausgenutzt und die Datenübertragung vorübergehend einkanalig über das jeweils noch als ordnungsgerecht angesehene Übertragungssystem betrieben; dies ist nach der Lehre der Erfindung zulässig, sofern die dabei übermittelten Daten durch zusätzliche Maßnahmen gegen nicht erkennbare Feh-

ler zusätzlich gesichert werden.

9 Patentansprüche

3 Figuren

Patentansprüche

1. Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mindestens zwei signaltechnisch nicht sicheren Ein/Ausgabebaugruppen, über die die Rechner des Mehrrechnersystems mindestens zweikanalig Datentelegramme von und/oder zu anderen Rechnern und/oder sonstigen datenaufnehmenden, abgebenden oder verarbeitenden Systemen übertragen und über die sie von dort in Form von inhaltlich übereinstimmenden Telegrammen für die Ein/Ausgabebaugruppen durch Prüfdaten gesicherte Nutzdaten empfangen bzw. nach dort abgeben, d a d u r c h g e k e n n z e i c h n e t ,
daß das sichere Mehrrechnersystem spätestens beim Erkennen von ihm von einer Datenquelle übermittelten ungleichen Daten in diesen Ein/Ausgabebaugruppen die dort abgelegten Daten einer Redundanzprüfung unterzieht und hieraus die Ein/Ausgabebaugruppe mit den fehlerhaften Daten bestimmt,
daß das sichere Mehrrechnersystem dann die weitere Auswertung bzw. Fortschaltung von Daten über diese Ein/Ausgabebaugruppe im Verkehr mit dem System, von dem die fehlerbehafteten Daten stammen, unterbindet,
daß das sichere Mehrrechnersystem die Datenquelle, von der es die ungleichen Daten erhalten hat, von dieser Maßnahme unterrichtet und diese Datenquelle dazu veranlaßt, die weitere Auswertung bzw. Fortschaltung von Daten über diejenige Ein/Ausgabebaugruppe, von der die als fehlerhaft erkannten Daten stammen, im Verkehr mit ihm zu unterbinden,
daß das sichere Mehrrechnersystem diese Datenquelle im Verkehr mit ihm zur Abgabe von höherredundanten Daten auf eine der von ihr noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppen veranlaßt und daß

sie das Einhalten der Redundanzbedingungen überwacht, daß das sichere Mehrrechnersystem auch selbst im Verkehr mit dem Datenempfänger der betreffenden Datenquelle die zu übertragenden Daten höherredundant erstellt, über eine der von ihm noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppen an den Datenempfänger übermittelt und den Datenempfänger zur Überwachung der Redundanzbedingungen veranlaßt, daß das sichere Mehrrechnersystem bei Nichteinhaltung der Redundanzbedingungen durch die in einer der noch von ihm betriebenen Ein/Ausgabebaugruppen abgelegten Daten auch die weitere Auswertung bzw. Fortschaltung der dort abgelegten Daten unterbindet und daß das sichere Mehrrechnersystem die weitere Auswertung und Fortschaltung der in einer seiner noch betriebenen Ein/Ausgabebaugruppen abgelegten Daten unterbindet, wenn seit dem ersten Feststellen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen eine definierte maximale Zeitdauer vergangen ist, ohne daß die Störung in der bzw. den als defekt erkannten Ein/Ausgabebaugruppen bzw. dem betroffenen Übertragungskanal behoben wurde.

2. Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mindestens zwei signaltechnisch nicht sicheren Ein/Ausgabebaugruppen, über die die Rechner des Mehrrechnersystems mindestens zweikanalig Datentelegramme von und/oder zu anderen Rechnern und/oder sonstigen Daten aufnehmenden, abgebenden oder verarbeitenden Schaltmitteln übertragen und über die sie von dort in Form von inhaltlich übereinstimmenden Telegrammen für die Ein/Ausgabebaugruppen durch Prüfdaten gesicherte Nutzdaten empfangen bzw. nach dort abgeben,

dadurch gekennzeichnet,
daß das sichere Mehrrechnersystem spätestens beim Erkennen von ungleichen Daten in diesen Ein/Ausgabebaugruppen die sort abgelegten Daten einer Redundanzprüfung unterzieht und hieraus die Ein/Ausgabebaugruppe mit den fehlerhaften Daten bestimmt,
daß das sichere Mehrrechnersystem dann die weitere Auswertung bzw. Fortschaltung von Daten über diese Ein/Ausgabebaugruppe unterbindet,
daß das sichere Mehrrechnersystem für die Dauer der Abschaltung einer seiner Ein/Ausgabebaugruppen die mit ihm kommunizierenden Datenquellen zur Abgaben von höherredundanten Daten auf eine der von ihm noch betriebenen auf einen anderen Kanal geführten Ein/Ausgabebaugruppen veranlaßt und das Einhalten der Redundanzbedingungen überwacht,
daß das sichere Mehrrechnersystem auch selbst im Verkehr mit Datenempfängern die zu übertragenden Daten höherredundant erstellt, über eine der von ihm noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppenan die Datenempfänger übermittelt und die Datenempfänger zur Überwachung der Redundanzbedingungen veranlaßt,
daß das sichere Mehrrechnersystem bei Nichteinhaltung der Redundanzbedingungen durch die in einer der noch von ihm betriebenen Ein/Ausgabebaugruppen abgelegten Daten auch die weitere Auswertung bzw. Fortschaltung der dort abgelegten Daten unterbindet
und daß das sichere Mehrrechnersystem die weitere Auswertung und Fortschaltung der in einer seiner noch betriebenen Ein/Ausgabebaugruppen abgelegten Daten unterbindet, wenn seit dem ersten Feststellen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen eine definierte maximale Zeitdauer vergangen ist, ohne daß die

Störung in der bzw. den als defekt erkannten Ein/Ausgabebaugruppen bzw. dem betroffenen Übertragungskanal behoben wurde.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das sichere Mehrrechnersystem beim Feststellen von ungleichen Daten in seinen mit inhaltlich gleichenDaten versorgten Ein/Ausgabebaugruppen und/oder beim Feststellen von Fehlern in den höherredundant gesicherten Daten vor dem bleibenden Sperren der Auswertung der in den jeweils betroffenen Ein/Ausgabebaugruppen abgelegten Daten mindestens eine erneute Datenübermittlung anfordert.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, daß das sichere Mehrrechnersystem beim Erkennen ungleicher Daten in den durch die inhaltlich gleichen Telegramme belegten Ein/Ausgabebaugruppen die weitere Auswertung bzw. die Fortschaltung von Daten aus den in den Vergleich jeweils einbezogenen Ein/Ausgabebaugruppen unterbindet, wenn die von ihm durchgeführten Redundanzprüfungen für die Daten in diesen Ein/Ausgabebaugruppen zu dem Ergebnis führen, daß die übermittelten Daten den Prüfbedingungen genügen.

5. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß das Mehrrechnersystem beim Erkennen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen mindestens die Datenquelle, von der die fehlerhaft abgelegten Daten stammen, davon unterrichtet, von welcher ihrer Ein/Ausgabebaugruppen diese Daten stammen und daß die betreffende Datenquelle daraufhin die weitere Ausgabe von Daten über diese Ein/Aus-

gabebaugruppe unterbindet und die Ausgabe höherredundanter Daten über eine ihrer dann noch betriebenen Ein/Ausgabebaugruppen auf einem anderen Kanal veranlaßt bzw. auch ihrerseits das Einhalten der vorgegebenen Redundanzbedingungen beim Datenempfang über diese Ein/Ausgabebaugruppe prüft.

6. Verfahren nach Anspruch 1, 2 oder 3, d a d u r c h g e k e n n z e i c h n e t , daß die maximale Zeitdauer für die Betriebsfortführung des Mehrrechnersystems ab dem ersten Feststellen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen abhängig gemacht ist von der für die noch betriebenen Ein/Ausgabebaugruppen zu erwartenden MTBF und der nach dem Auftreten der Störung gewählten Datenredundanz.

7. Verfahren nach Anspruch 1, 2 oder 3, d a d u r c h g e k e n n z e i c h n e t , daß die höherredundanten Daten durch Verdoppelung der Datentelegramme und antivalente Darstellung der Daten in aufeinanderfolgenden Telegrammen gebildet sind.

8. Einrichtung zur Durchführung des Verfahrens nach mindestens einem der Ansprüche 1 bis 7, d a d u r c h g e k e n n z e i c h n e t , daß für die Datenübertragung ein mindestens zweikanaliges Bussystem (B1, B2) vorgesehen ist und daß die zur Aufnahme jeweils inhaltlich gleicher Datentelegramme vorgesehenen Ein/Ausgabebaugruppen (z.B. E/A21, E/A22) des sicheren Mehrrechnersystems(RS2) an verschiedene Kanäle (B1 bzw. B2) des Bussystems angeschlossen sind.

9. Einrichtung zur Durchführung des Verfahrens nach Anspruch 6, d a d u r c h g e k e n n z e i c h n e t, daß das sichere Mehrrechnersystem (R1, R2) ein signaltechnisch sicheres Zeitglied (T1, T2) aufweist, das beim Sperren der Auswertung von in einer Ein/Ausgabebaugruppe abgelegten Daten einstellbar ist, nach Ablauf der ihm eingeprägten Schaltzeit die Auswertung der höherredundant gesicherten Daten unterbindet und das beim Feststellen von Übertragungs- oder Speicherfehlern in diesen höherredundant gesicherten Daten die Auswertung dieser Daten unterbindet.

(1/2)

FIG 1

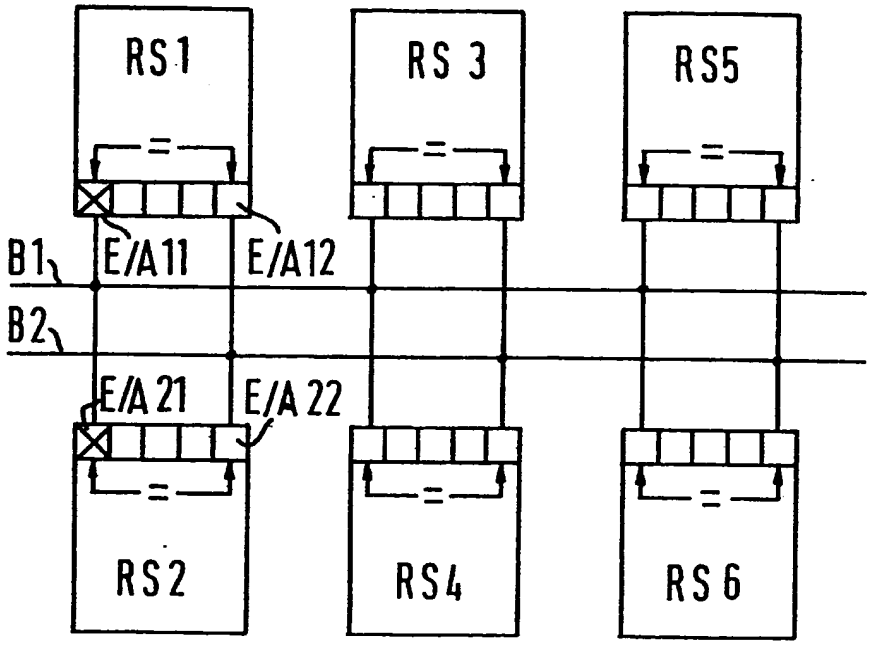

RS 1
RS 3
RS 5
B1
E/A 11
E/A 12
B2
E/A 21
E/A 22
RS 2
RS 4
RS 6

FIG 2

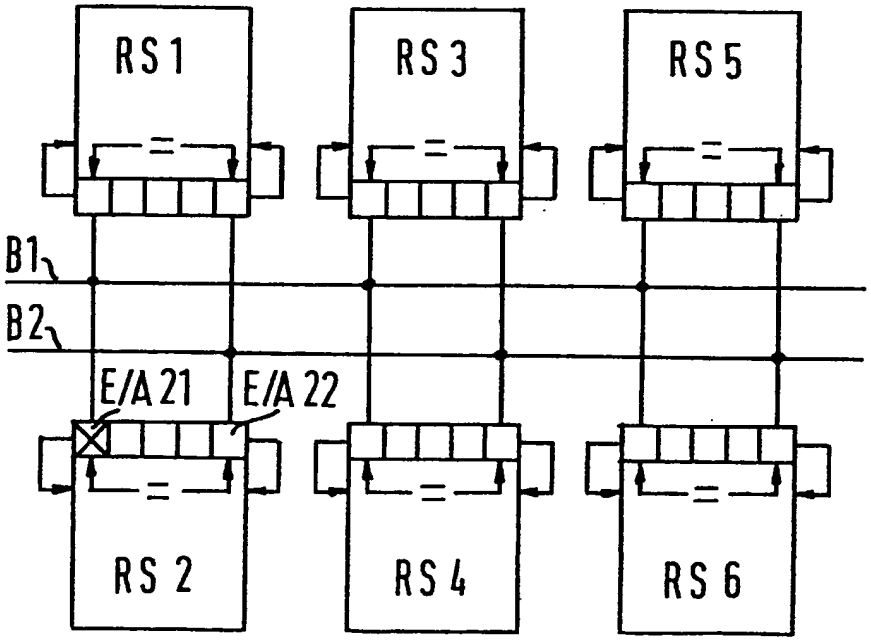
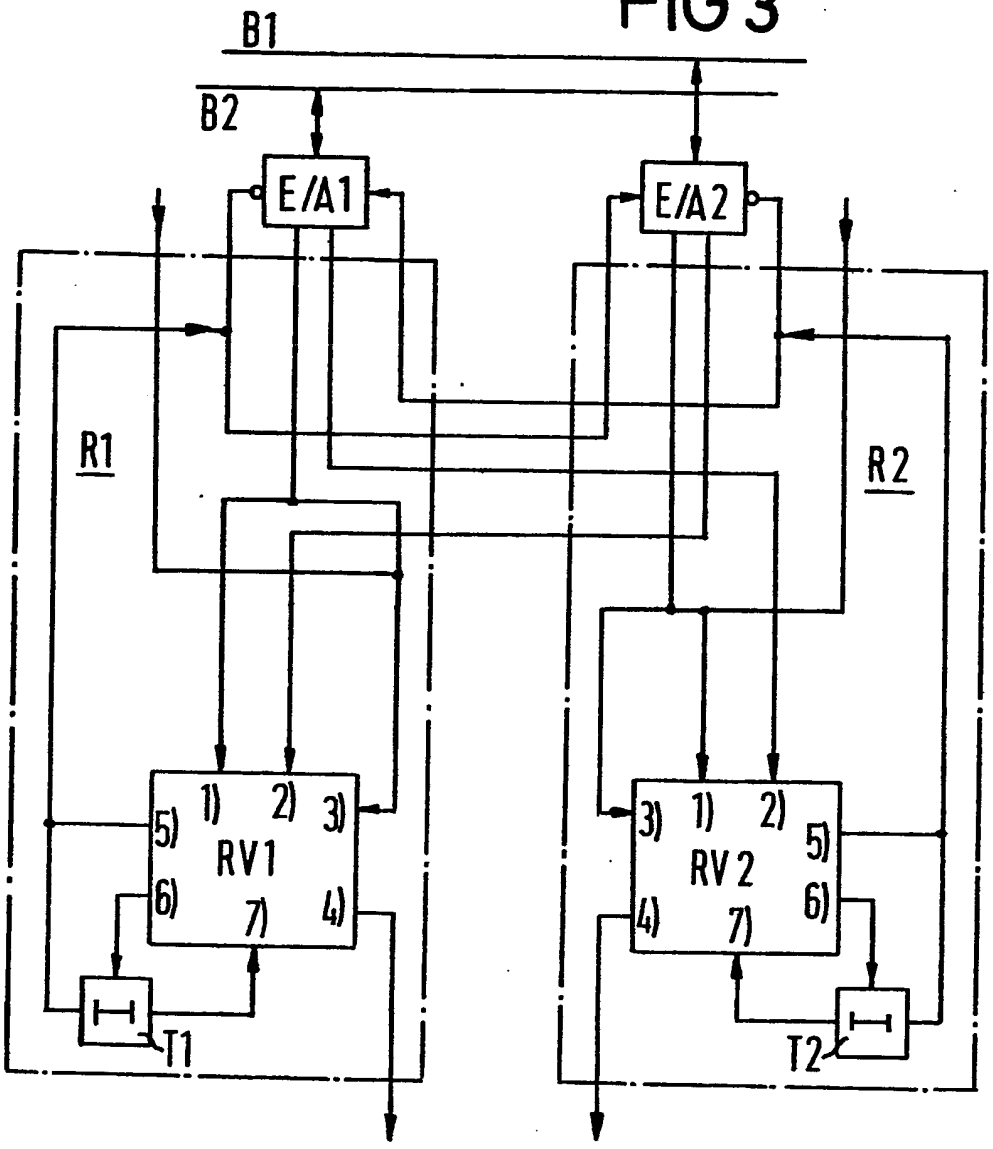

RS 1
RS 3
RS 5
B1
B2
E/A 21
E/A 22
RS 2
RS 4
RS 6

FIG 3



1)
2) DATENVERGLEICH; REDUNDANZPRÜFUNG
3) DATENEINGABE
4) DATENAUSGABE
5) SPERREN DER DATENAUSWERTUNG, ANFORDERN HÖHERREDUNDANTER DATEN, EINSTELLEN DES ZEITGLIEDES
6) RÜCKSTELLEN DES ZEITGLIEDES
7) ABBRUCH DES DATENVERKEHRS

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.